ZIMPERIUM

Why the Software Bill Of Materials(SBOM) Must Extend to the Mobile App Supply Chain

Supply Chain attacks are not a new problem, but their frequency has been increasing since 2013 when Target was breached. But the recent attacks on SolarWinds Orion, Kaseya VSA, Accellion, Microsoft have highlighted the fact that cybercriminals have shifted their focus from the primary targets to their suppliers. Why? Because cybercriminals are aware of the over-reliance on open source and commercial software components and its upkeep in the public and private sector.

But what most fail to realize is this third-party dependency is not just in the form of IT infrastructure management solutions but also in third-party components used across millions of mobile applications. **50-90% of client-side executing code on websites and mobile apps is from third parties.** Determining whether each third party update is required and safe gets expensive and difficult very quickly. And unfortunately the marketplace does not demand this level of scrutiny allowing organizations to trade this due diligence for faster feature development.

Research shows that in the first quarter of 2021 alone, **supply chain attacks rose by 42%**, impacting 7 million people. During this time, 137 organizations reported their supply chains were attacked and at 27 different third-party vendors. The European Union Agency for Cybersecurity mapping on emerging supply chain attacks finds **66% of attacks focus on the supplier's code.** Today, organizations globally have realized that it's no longer sufficient to secure their enterprise. They need to think about their supply chain and its associated risks.

This shift to supply chain attacks makes sense for two key reasons. First, software developers create products by assembling existing open source and commercial software components to accelerate speed to market. But in most cases, they are unaware of the third-party's security protocol. Second, developers do not update these components 80% of the time as they can't keep up with the updates and don't want to fix something that's not broken. Unfortunately, cybercriminals and hacker groups are aware of this behavior and target the same third-party code to steal sensitive data, redirect to sites with malware, takeover devices, and much more.

50-90%
of client-side executing code on websites and mobile apps is from 3rd parties

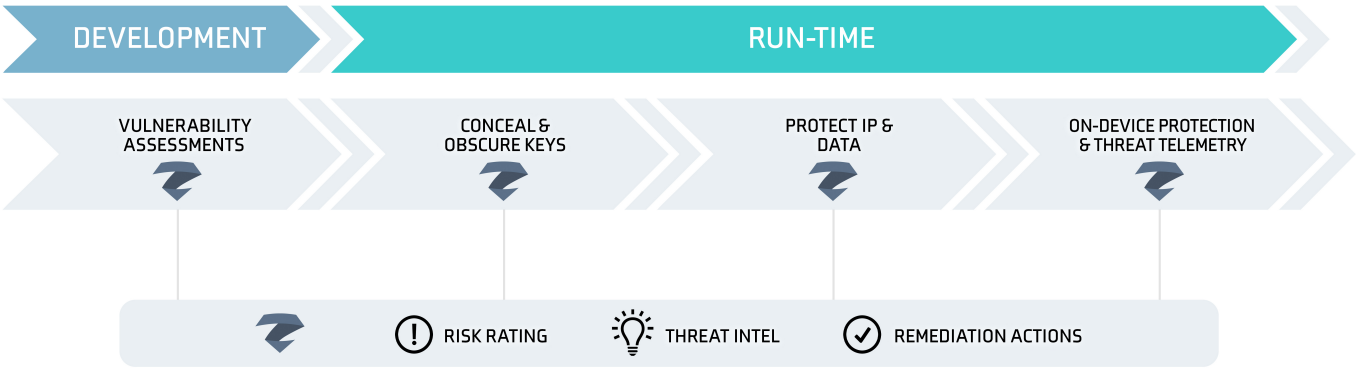
42%
Amount supply chains rose in Q1 2021

66%
of attacks focused on supplier's code

Software supply chain attacks are effective as they focus on finding the weakest third-party component and then exploiting it. The most recent attacks impacted Fortune 500, US Military, the Pentagon, the State Department, and many more, prompting the White House to issue an executive order to better protect the nation's digital infrastructure in public and private sectors. By laying out new federal Software Bill of Materials (SBOM) standards, the order aims to bring more transparency into the ingredients of open source and commercial software components.

The SBOM will be helpful to those who develop or manufacture software, select or purchase software, and operate the software. Buyers can use an SBOM to perform vulnerability analysis to evaluate risk in a product and the associated third-party components. SBOMs will quickly and easily help organizations determine whether they are at risk when new vulnerabilities are discovered.

All software developers will have to comply with the Executive Order for agencies to continue using their software and selling it to government agencies. Government agencies that build their software or outsource development to systems integrators will also have to comply.



Zimperium, a leading mobile-security company, is helping organizations build secure and compliant mobile applications. It is the only unified solution that combines comprehensive in-app protection with centralized risk visibility.

With the platform, organizations can gain visibility into any vulnerabilities within their mobile apps. The binary analysis of the application inspects native and third-party components to find security vulnerabilities, privacy gaps, and compliance violations. This visibility helps organizations better understand the risks in their mobile apps and the underlying third-party components and meet new federal SBOM standards. Eliminating supply chain attacks is not realistic, but our goal is to ensure organizations are better prepared to respond in a timely manner when they do.

Contact us to learn more about how Zimperium can help you automate and integrate SBOMs into your vulnerability management programs.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244